SNMP

Simple Network Management Protocol

Administración de la red

ISO divide la administración de la red en cinco partes que se definen dentro del Modelo OSI:

- **Administración de la contabilidad:** Proporciona información sobre costos y los usos contables.
- **Administración de la configuración:** Administra la configuración real de la red.
- **Administración de fallos:** Detecta, aísla y corrige los fallos, incluyendo el mantenimiento de un registro y un diagnóstico de los errores.
- **Administración del desempeño (prestaciones):** Mantiene una eficiencia y un desempeño máximos, incluyendo la recopilación de estadísticas y el mantenimiento de registros para definir un **"*baseline*"**
- **Administración de la seguridad:** Mantiene un sistema seguro y administra el acceso.

Administración en TCP/IP

El Comité Asesor de Internet (Internet Advisory Board, IAB) ha elaborado o adoptado varias normas para la administración de la red. En su mayoría, éstas se han diseñado específicamente para ajustarse a los requisitos de TCP/IP, aunque cuando es posible cumplen con la arquitectura OSI. Para cubrir dichas necesidades se han creado dos protocolos, ambos con funcionalidades parecidas:

1.-SNMP: comprende el uso del Protocolo Simple para Administración de la Red (Simple Network Management Protocol, **SNMP**).

2.-TCP/IP(CMOT): comprende las normas OSI para administración de la red, llamados Servicios Comunes de Información sobre la Administración (Common Management Information Services, CMIS), y al Protocolo Común de Información sobre la Administración (*Common Management Information Protocol, CMIP*). IAB ha publicado "**C**ommon **M**anagement Informatíon Servíces and protocol **O**ver **TCP/IP(CMOT)"** como una norma para TCP/IP y para la administración OSI.

SNMP

SNMP es un protocolo de nivel de aplicación para consulta a los diferentes elementos que forma una red, (*routers, switches, hubs, hosts, modems, impresoras, etc*).

Cada equipo conectado a la red ejecuta unos procesos (**agentes**), para que se pueda realizar una administración tanto remota como local de la red. Dichos procesos van actualizando *variables* (especie de históricos) en una base de datos, que máquinas remotas pueden consultar.

Por ejemplo, en el caso de:

*-un **router**: interfaces activos, la velocidad de sus enlaces serie, número de errores, bytes emitidos, bytes recibidos, ...*

*-en una **impresora**: que se terminó el papel, ...*

*-en un **modem**: la pérdida de conexión, etc*

*-en un **switch**: bocas conectadas, desconectar un boca en el caso de Ips duplicadas, si la máquina está infectada de virus, etc*

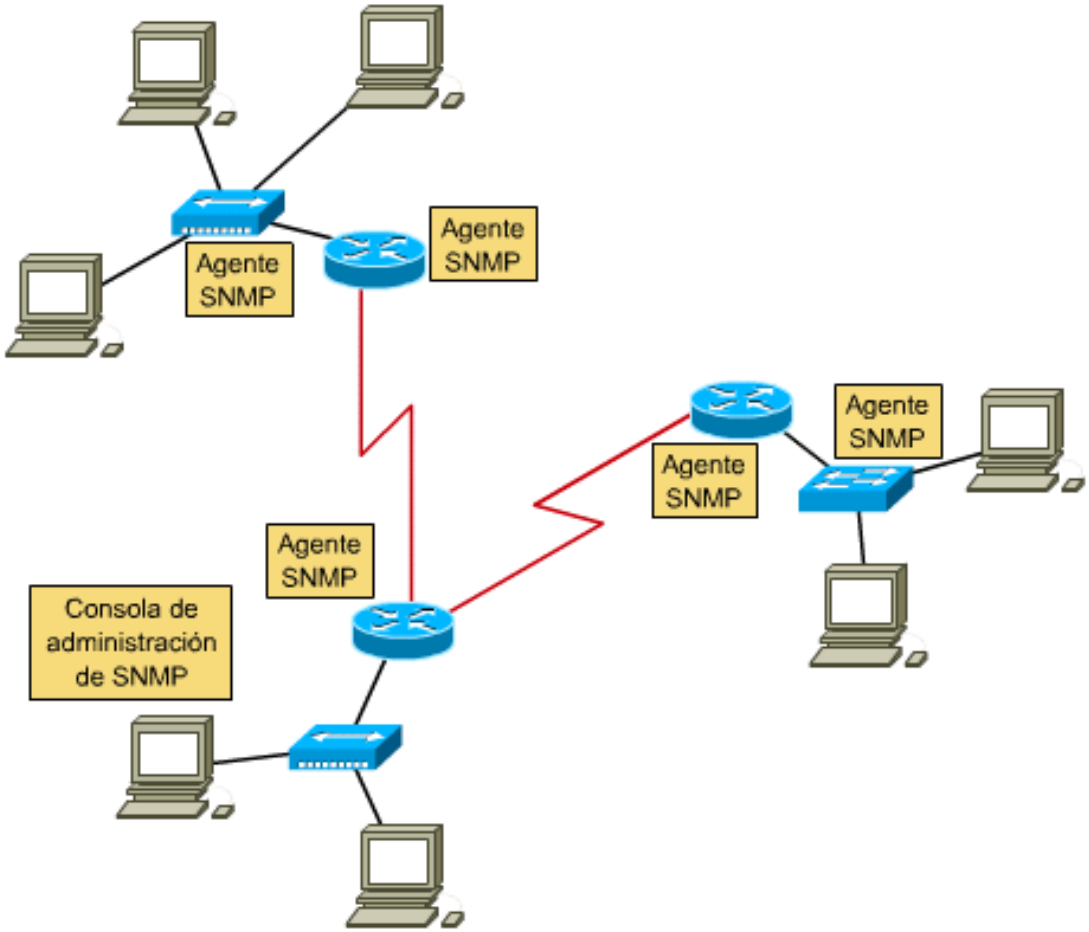
SNMP: arquitectura

La Arquitectura de Administración de Red se compone de cuatro componentes principales:

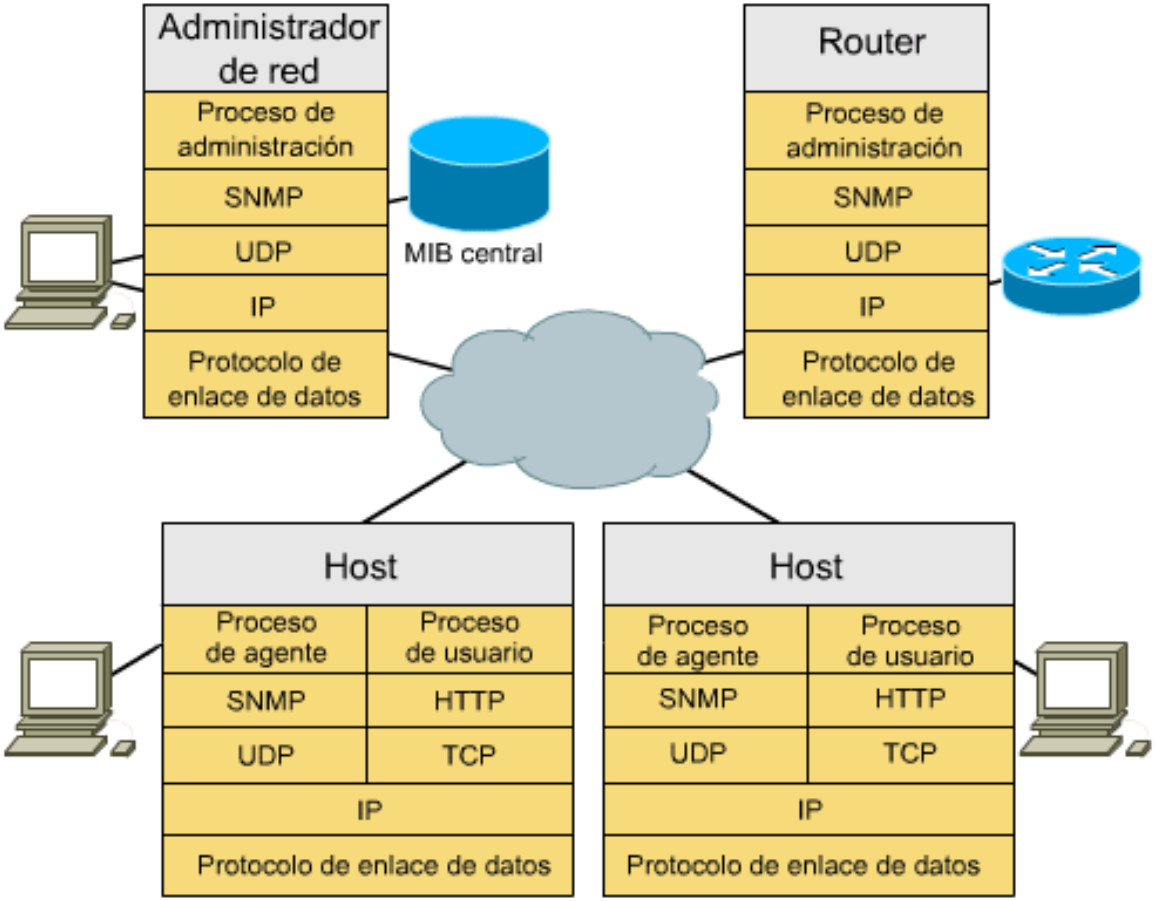
- estación de administración
- agente de administración del dispositivo administrado
- base de información de administración,
- protocolo de administración.

SNMP facilita la comunicación entre la estación administradora y el agente de un dispositivo de red (o nodo administrado), permitiendo que los agentes transmitan datos estadísticos (*variables*) a través de la red a la estación de administración.

Agentes SNMP



Componentes de la arquitectura SNMP



SNMP: funcionamiento

La forma normal de uso del SNMP es:

1.- **Pregunta**: que la estación administradora envíe una solicitud a un agente (proceso que atiende petición SNMP) pidiéndole información o mandándole actualizar su estado de cierta manera. Este método se conoce como ***sondeo***.

2.- **Respuesta**: la información recibida del agente es la respuesta o la confirmación a la acción solicitada.

El problema del sondeo que se incrementa con los nodos administrados y en ocasiones puede llegar a **perjudicar el rendimiento de la red**.

Interrupción: Es mejor que un agente pueda mandar la información al nodo administrador puntualmente, ante una situación predeterminada, por ejemplo una anomalía detectada en la red. Este método es conocido como ***interrupción***.

SNMP: protocolos

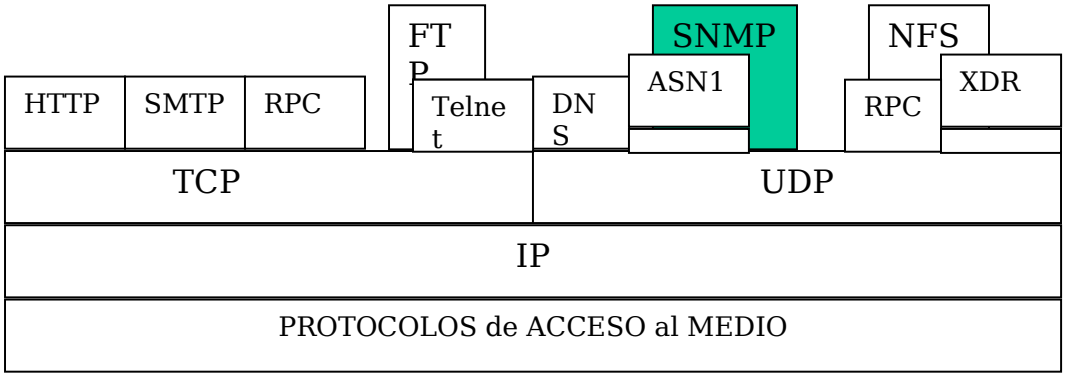
SNMP es independiente del protocolo (IPX de SPX/IPX de Novell, IP con UDP)

SNMP se puede implementar usando comunicaciones UDP o TCP, pero por norma general, se suelen usar comunicaciones UDP en la mayoría de los casos. Con UDP, el protocolo SNMP se implementa utilizando los puertos 161 y 162.

- *puerto 161 se utiliza para las transmisiones normales de comando SNMP*
- *puerto 162 se utiliza para los mensajes de tipo "trap" o interrupción.*

Pila de protocolos en SNMP para TCP/IP

(SNMP trabajo también sobre IPX, Appletalk,..)



Formato de representación de la información: Abstract Syntax Notation.1 (ASN1)que define la sintaxis específica para el intercambio de información independientemente del dispositivo que la procesa, similar a XDR (eXternal Data Representation) en RPCs

Elementos de la arquitectura SNMP

- *Nodos administrados que ejecutan agentes SNMP y estación administradora*
- *Estructura e identificación de la información sobre la administración (SMI)* : Una especificación que permite definir las entradas en una MIB.
- *Base de información de la administración (MIB)* : Una base de datos relacional (*organizada por objetos (o variables) y sus atributos (o valores)*) que contiene información del estado y es actualizada por los agentes.
- *Protocolo simple para administración de la red (SNMP)*: El método de comunicación entre los dispositivos administrados y los servidores.

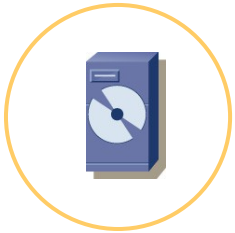
Componentes de SNMP

Estación de administración es la interface del administrador de red en el sistema. Contiene el sw de gestión, y mantiene una base de datos denominada MIB con formato SMI.

Agente de administración es el proceso de los dispositivos que están siendo monitorizados. Puentes, routers, hubs, and switches

SNMP
UDP
IP
MEDIA ACCESS

Protocolo de administración: protocolo de capa de aplicación diseñado para comunicar entre el Administrador y el Agente.



BASE DE DATOS DE ADMINISTRACIÓN: Aunque no es imprescindible es interesante disponer de una BD en la que ir volcando los históricos y toda la información obtenida de las MIB.

SMI: Structure o Management Information

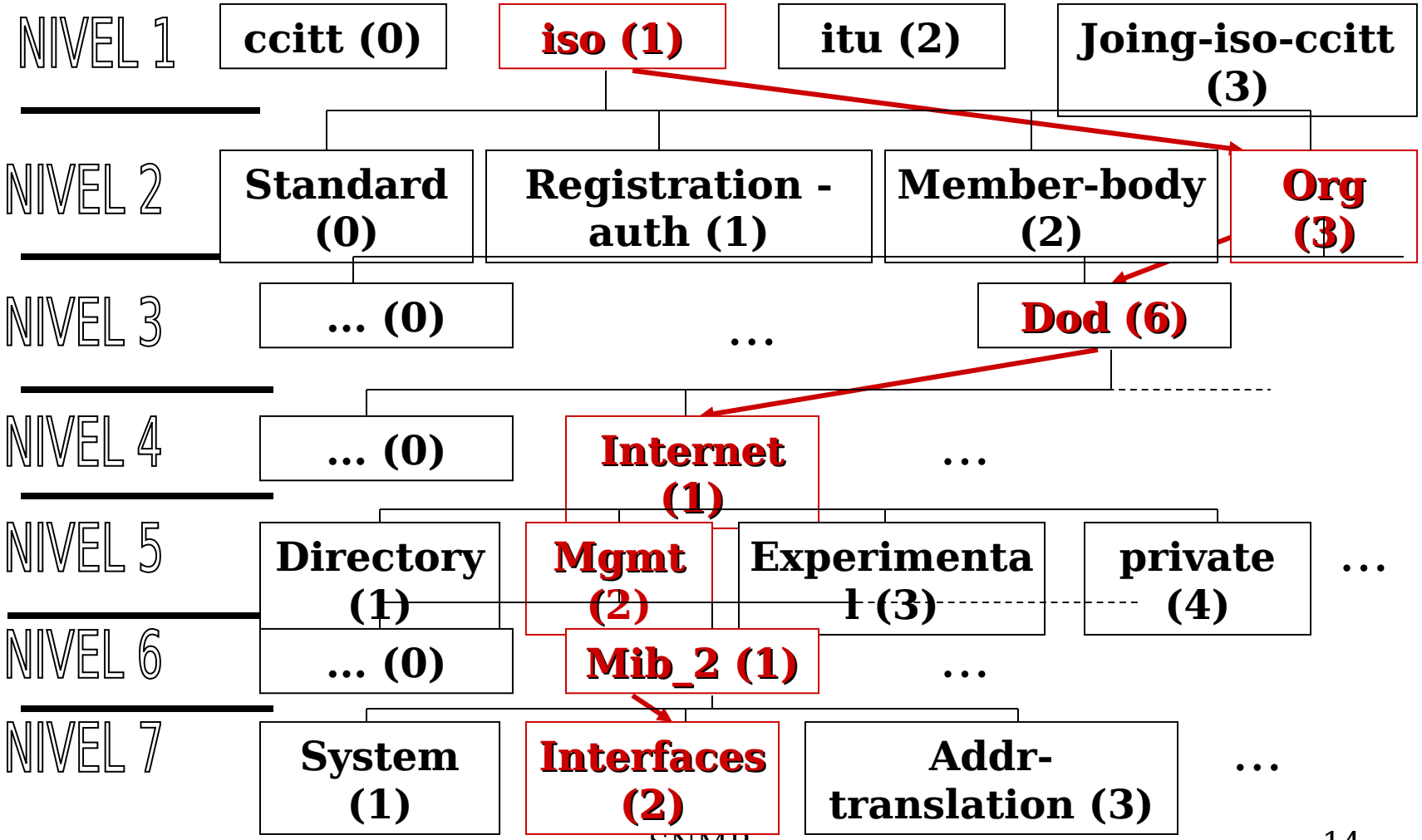
SMI presenta una **estructura en forma de árbol global** para la información de administración, convenciones, sintaxis y las reglas para la construcción de MIBs.

La MIB está organizada en **niveles**, que a su vez lo hace en **módulos** que contienen **grupos** de variables interrelacion

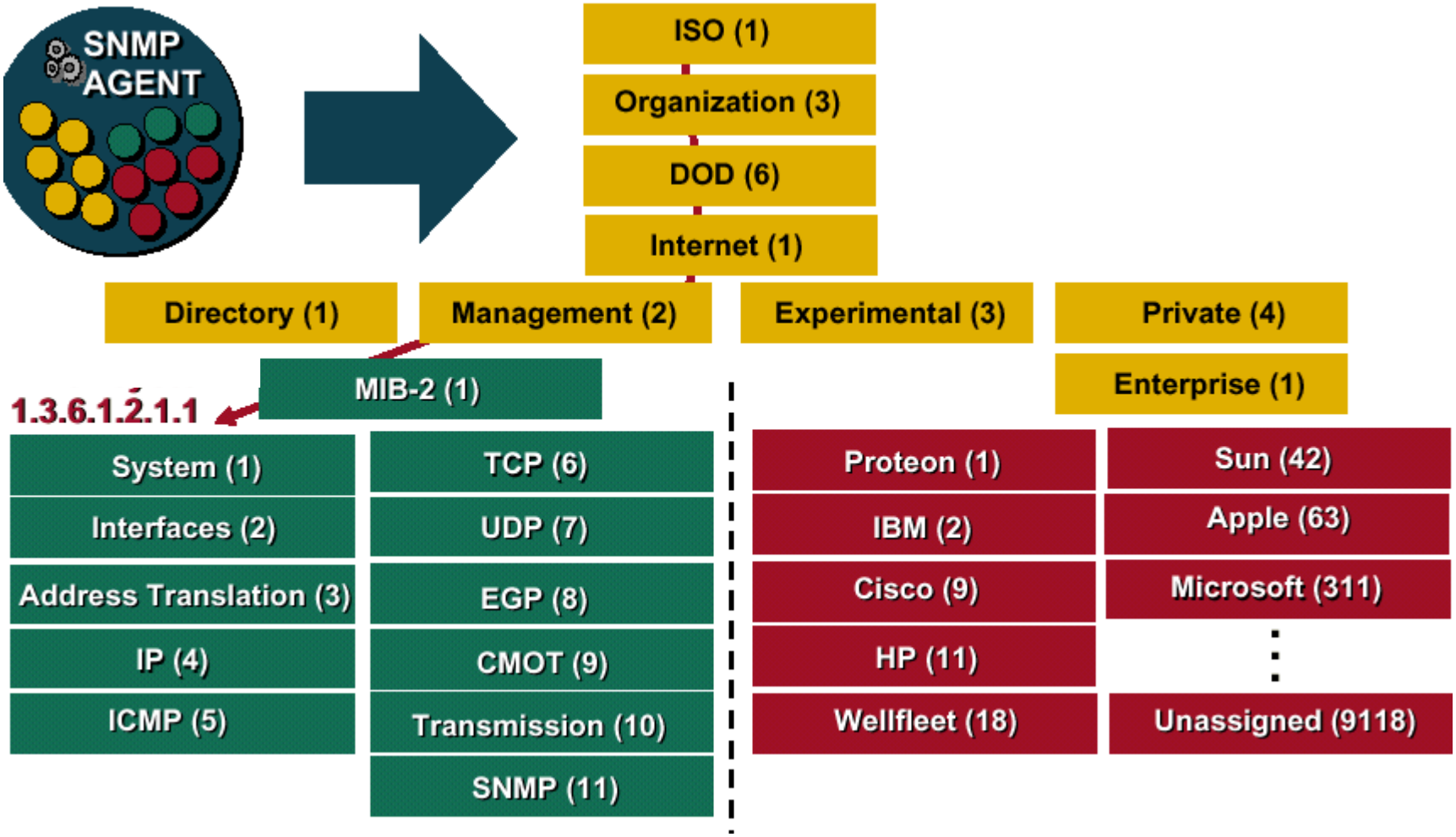
Nota: la estructura SMI guarda similitud con el **DNS** y sus zonas de autoridad, o variables definidas por cada fabricante.

Ejemplo de GRUPOS de variables en MIB-2 en la SMI: **System** (identifica el hw y sw), **AT** (traducción de direccíon de Ethernet a IP), **IP** (contador de paquetes, fragmentación), **ICMP** (contador de cada tipo de mensaje ICMP), **TCP** y **UDP** (conexiones abiertas TCP), **EGP** (estadística de protocolo externo)

Ejemplo de SMI para acceder a
Mib_2.Interfaces



Subarboles de la MIB-2



Ejemplo de codificación de objetos según SMI

iso.org.dod.internet.mgmt.mib_2.interfaces.iftable.ifEntry.variable.puerto

O su equivalente ***.1.3.6.1.2.1.2.2.1.variable.puerto***

Este formato para la representación de variables puede ser expresadas tanto en ASCII como números separados por puntos, en una notación intermedia entre ASCII y ASN1 conocida como OID (*Object Identifier*) o descriptor.

En esta notación inicialmente se identifica el organismo de estandarización, ISO y dentro de éste está ORG y dentro DOD (*Departamanet of Defense*), donde la primera rama del árbol desde DOD es Internet.

Así sucesivamente hasta especificar la variable (u objeto) y el puerto a consultar.

Objetos utilizados para monitorizar una interfaz Ethernet (1/2)

ifOperStatus:

Nos indica el estado operacional de un determinado enlace.

ifAdminStatus:

Se utiliza para cambiar el estado operacional de un enlace. Únicamente es accesible por el administrador de la red.

ifInErrrors:

Nos indica el número de paquetes entrantes en los que el agente ha encontrado algún tipo de error.

ifInDiscards:

El número de paquetes entrantes que el agente ha seleccionado para ser eliminados. No necesariamente son solo los que contienen errores. Una razón para eliminar paquetes suele ser liberar espacio en los buffers de entrada.

ifInOctets:

Indica el número total de bytes recibidos en el enlace.

Objetos utilizados para monitorizar una interfaz Ethernet (2/2)

ifOutErrors:

Indica el número total de paquetes que no han podido ser enviados por causa de un error.

ifOutDiscards:

El número de paquetes salientes que el agente ha seleccionado para ser eliminados. Además de aquellos que contienen algún error, también se eliminan para liberar espacio en los buffers de salida.

ifOutOctets:

El número total de octetos transmitidos fuera del enlace.

ifSpeed:

Nos da una estimación del ancho de banda actual que dispone el enlace en bits por segundo. En aquellos enlaces en los que el ancho de banda no varíe o en los que no sea posible hacer una aproximación exacta, este objeto suele contener el ancho de banda nominal

Base de información de administración (MIBs: **database of management information**)

La base de información de administración tiene una <u>estructura de base de datos (según SMI)</u> **y reside en cada dispositivo administrado**.

La base de datos contiene una serie de objetos (variables), que son datos sobre recursos reunidos en el dispositivo administrado.

OBJETO (o variable)

- Parámetro que corresponden a un grupo del dispositivo administrado: ***System, AT, IP, TCP, UDP, EGP, ...***
- POSEE ATRIBUTOS (o valores) QUE REPRESENTAN EL ESTADO DEL OBJETO
- LOS UNICOS METODOS QUE OPERAN SOBRE LOS ATRIBUTOS SON **ESCRIBIR Y LEER**
- LA SINTAXIS UTILIZADA PARA REPRESENTAR LA INFORMACION ES ASN.1
- ES UN SUBCONJUNTO DE SMI

Nodos administrados (agentes) (1/2)

Los periféricos que tienen integradas las capacidades para SNMP corren un paquete pequeño de software **agente** para administración (*generalmente de 64kB*), cargado como parte de un ciclo de arranque o guardado en la memoria fija (firmware) del dispositivo.

Estos dispositivos que tienen agentes SNMP se dice que se tratan de dispositivos o nodos administrados.

NO TODOS LOS NODOS SON AGENTES, NI PUEDEN SERLO.

Agente Apoderado (o *proxy*): GESTIONA LOS DISPOSITIVOS QUE NO PUEDEN EJECUTAR UN AGENTE LOCAL. LOCALIZACION: EXTERNO AL DISPOSITIVO ADMINISTRADO.

Nodos administrados (agentes) (2/2)

Los dispositivos administrados por SNMP (puentes, routers, hubs y switches) se comunican con el software servidor SNMP que está localizado en cualquier parte de la red y les permitan ser controlados por la estación de administración.

El agente de administración responde a la estación de administración de dos maneras:

- ***mediante sondeo o pooling****: la estación de administración requiere datos desde el agente y el agente responde con los datos solicitados*
- ***por interrupción****: tal que se establecen umbrales (límites superiores o inferiores) en el dispositivo administrado y si se supera este umbral en el dispositivo, envía un mensaje de alerta a la estación de administración*.

En ocasiones se puede combinar ambos métodos, conocido como sondeo dirigido a interrupción.

Estación de administración

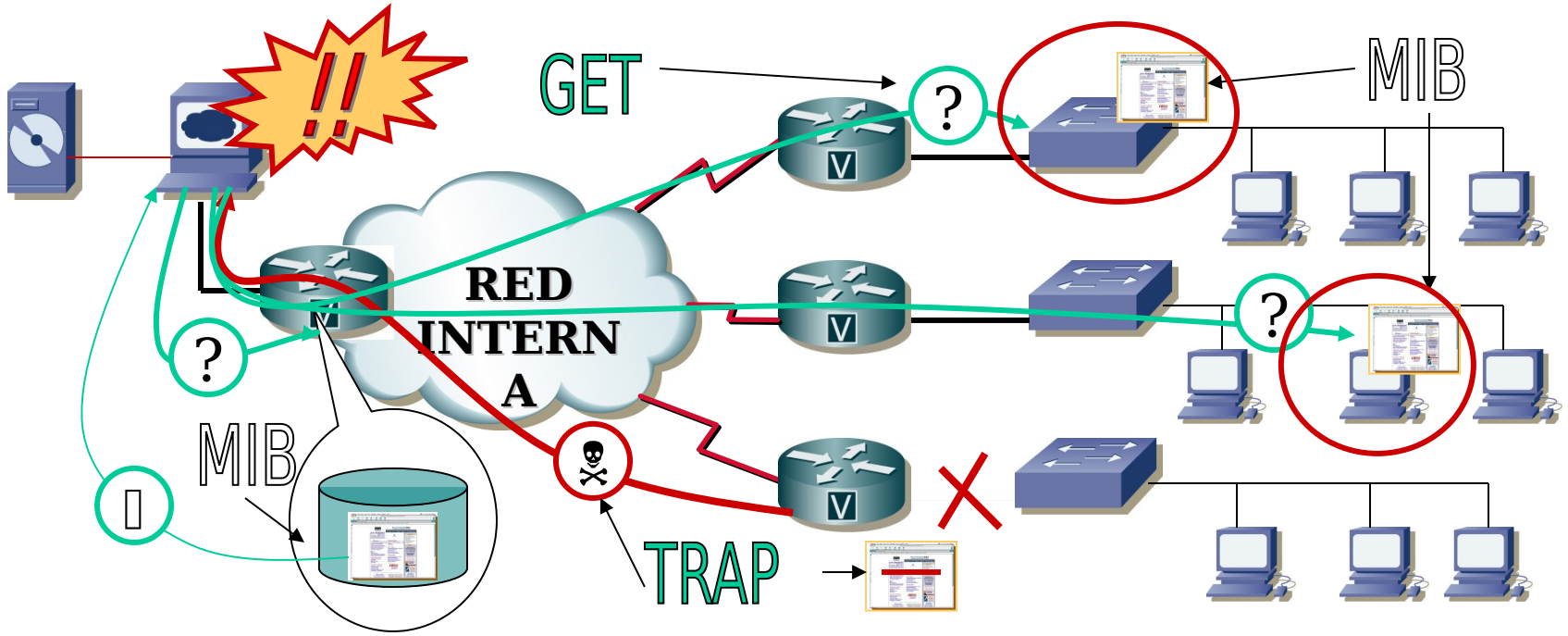
La estación de administración es la interfaz del administrador de red al sistema de red. Posee los programas para manipular los datos y controlar la red. La estación de administración también mantiene una base de datos de información de administración (MIB) extraída de los dispositivos bajo su administración.

Consola de administración

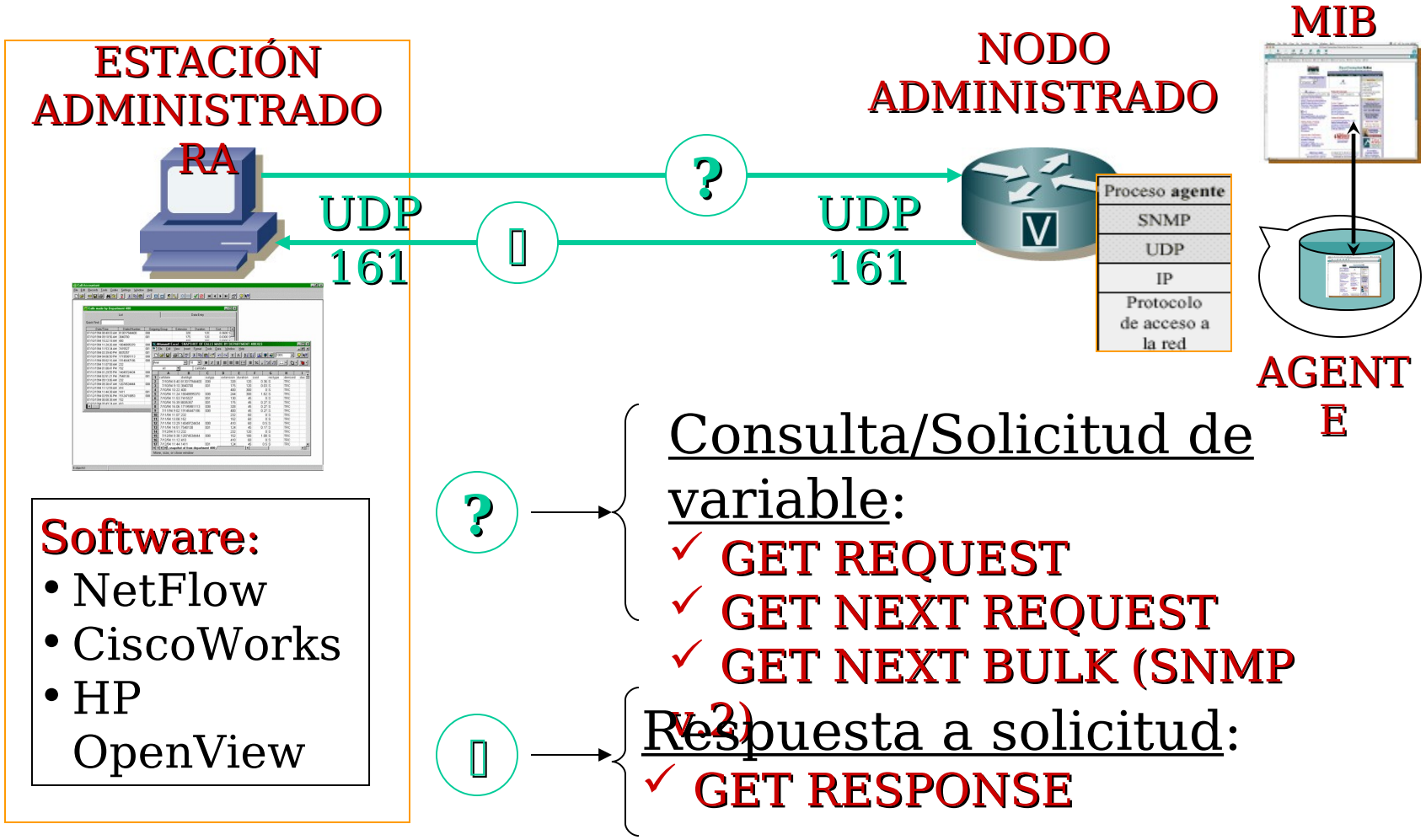
SNMP es un protocolo de capa de aplicación diseñado para comunicar datos entre la consola de administración y el agente de administración. Los comandos básicos que ejecuta son:

- *OBTENER (GET),* que implica que la consola de administración **recupera datos del agente**
- *COLOCAR (PUT),* que implica que la consola de administración **establece los valores de los objetos en el agente**
- *CAPTURAR (TRAP),* que implica que el agente notifica a la consola de administración acerca de los sucesos de importancia por **interrupción**

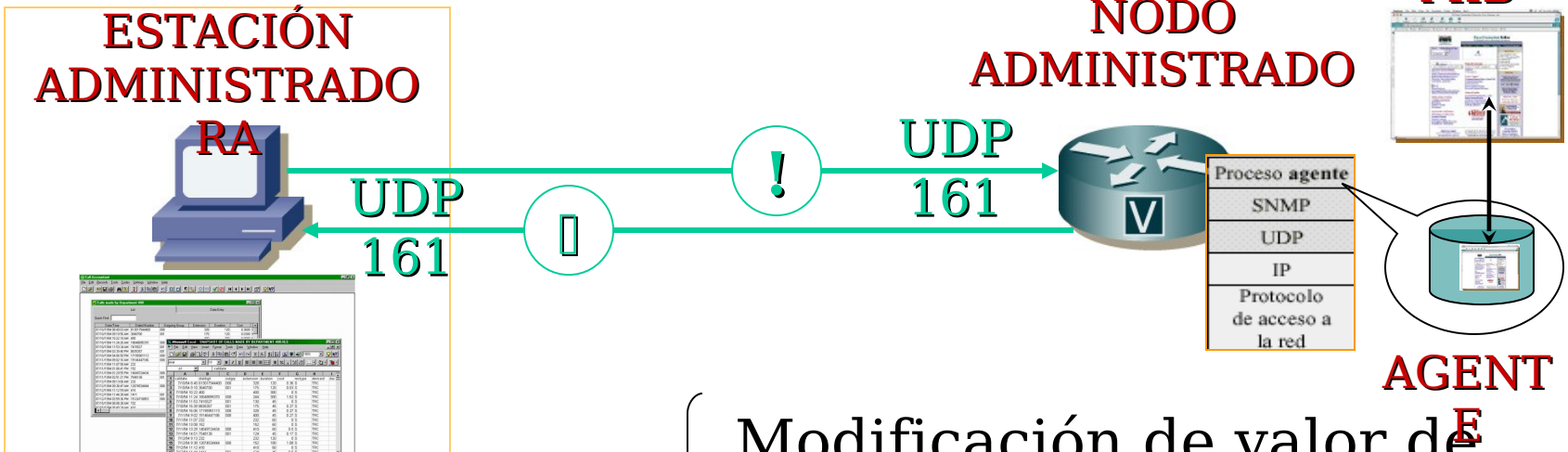
Ejemplo funcionamiento protocolo SNMP



Obtención de información



Modificación de información



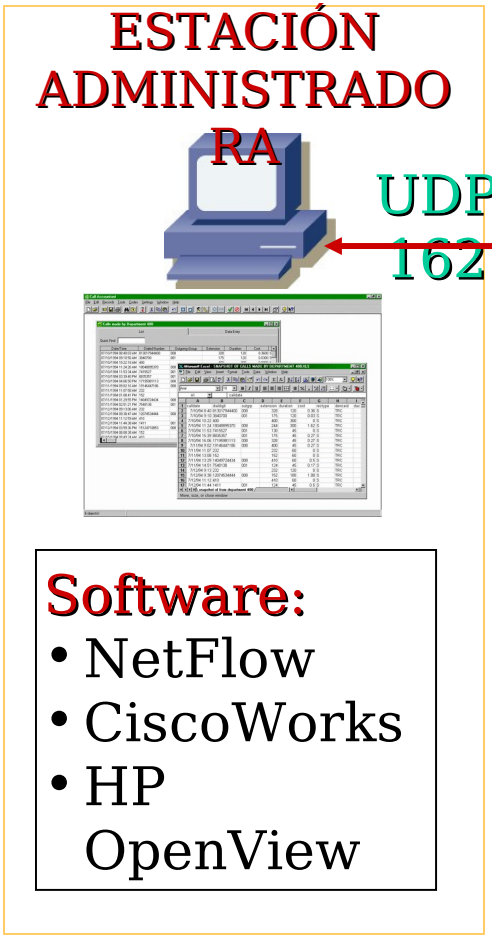
Software:
- NetFlow
- CiscoWorks
- HP OpenView

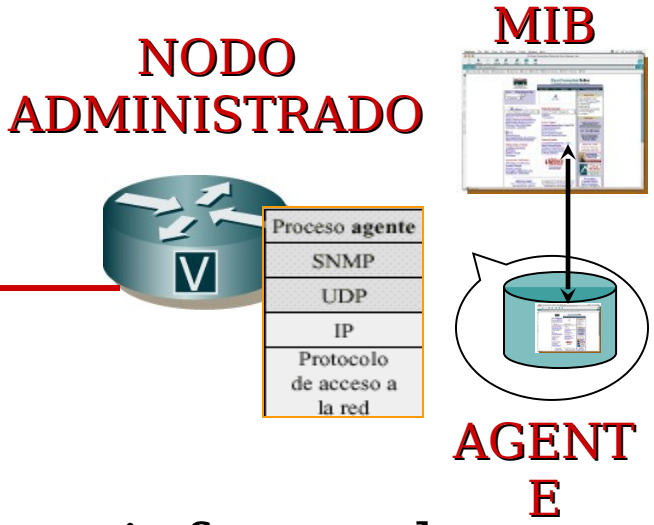
!

Modificación de valor de variable:
- ✓ **SET REQUEST**
- ✓ **SET NEXT REQUEST**

EJEMPLO: Se puede usar para resetear el valor de los contadores, como el número de paquetes procesados.

Generación de interrupciones





Software:
- NetFlow
- CiscoWorks
- HP OpenView

<u>Un Agente informa de un evento</u>:
- ✓ **TRAP**

EJEMPLO: El Agente de un router informa de que un enlace ha caído.

PRIMITIVAS

El SNMP define ocho mensajes que pueden enviarse:

1. GET REQUEST
2. GET NEXT REQUEST
3. GET BULK REQUEST (en SNMP v2)
4. SET REQUEST
5. SET NEXT REQUEST
6. GET RESPONSE
7. TRAP
8. INFORM REQUEST (en SNMP v2)

La implementación de cada uno de estos mensajes lo tenemos en Linux a través de las siguientes funciones: *snmpget, snmpgetnext, snmpgetbulk* y *snmpset*.

GET REQUEST

- SOLICITA UNO O MAS (lista) ATRIBUTOS (valores) DE UN OBJETO (o variable).
- TRANSMITIDA POR EL NODO ADMINISTRADOR
- RECIBIDA POR EL AGENTE QUE CONTESTA

GET NEXT REQUEST

- SOLICITA EL SIGUIENTE ATRIBUTO DE UN OBJETO
- TRANSMITIDA POR EL NODO ADMINISTRADOR
- RECIBIDA POR EL AGENTE QUE CONTESTA

GET BULK REQUEST

- SOLICITA UN CONJUNTO AMPLIO DE ATRIBUTOS EN VEZ DE SOLICITAR UNO A UNO
- TRANSMITIDA POR EL NODO ADMINISTRADOR
- RECIBIDA POR EL AGENTE

SET REQUEST

- ACTUALIZA UNO O VARIOS ATRIBUTOS DE UN OBJETO
- TRANSMITIDA POR EL NODO ADMINISTRADOR
- RECIBIDA POR EL AGENTE

SET NEXT REQUEST

- ACTUALIZA EL SIGUIENTE ATRIBUTO DE UN OBJETO
- TRANSMITIDA POR EL NODO ADMINISTRADOR
- RECIBIDA POR EL AGENTE

GET RESPONSE

- DEVUELVE LOS ATRIBUTOS SOLICITADOS
- TRANSMITIDA POR EL AGENTE
- RECIBIDA POR EL NODO ADMINISTRADOR

TRAP

- INFORMA FALLOS COMO LA PERDIDA DE COMUNICACION CON UN VECINO
- TRANSMITIDA POR EL AGENTE
- RECIBIDA POR EL NODO ADMINISTRADOR

INFORM REQUEST

- DESCRIBE LA BASE LOCAL DE INFORMACION DE GESTION MIB PARA INTERCAMBIAR INFORMACION NODOS DE ADMINISTRACION ENTRE SI
- TRANSMITIDA POR EL NODO ADMINISTRADOR
- RECIBIDA POR OTRO NODO ADMINISTRTADOR

CONCEPTO de INTERRUPCION

- INFORME DE UN SUCESO SIGNIFICATIVO
- TRANSMITIDO POR EL AGENTE
- RECIBIDO POR EL NODO ADMINISTRADOR

Monitorización inteligente

Ejemplo 1:

Mediante SNMP, un router puede reportar **un incremento de la carga cada 10 %.**

*"Si utiliza un sondeo dirigido por interrupción y se conoce la **carga del sondeo regular**, puede dar instrucciones al router para enviar una interrupción cuando se experimente un incremento significativo en la carga,10%"*

Después de recibir un mensaje de interrupción, el servidor puede seguir sondeando al dispositivo para mayores detalles.

Ejemplo 2:

Otro caso de configuración, cuando el router de salida con acceso a Rediris tiene tráfico de salida superior a 34 Mbps, que mande al administrador de la red notificación o alerta

Problema: SNMP y congestión

La monitorización se realiza por la propia red, por tanto si la red está congestionada, puede conllevar más problemas.

Si existe una fallo general en cualquier parte de la red (p.ej **fallo de la corriente eléctrica**), cada dispositivo administrado por SNMP tratará de enviar al mismo tiempo, mensajes controlados por interrupción hacia el servidor, para reportar el problema. Esto puede congestionar la red y producir una información errónea en el servidor.

SNMP: Versión 2 y 3

Versión 2:

De SNMPv1, para reducir la carga de tráfico adicional para la monitorización (con los GetBulk e Informs) y solucionar los problemas de monitorización remota o distribuida (con las RMON), ha dado paso a una nueva versión v2 en 1993.

Las versiones de SNMP son compatibles, en el sentido que SNMPv2 puede leer SNMPv1.

Versión 3:

SNMPv1 utiliza como mecanismo de autenticación (validación) un parámetro llamado “comunidad”, *de forma que si agente y estación administradora lo conocen, pueden interactuar*. Pero esta protección es muy debil porque el texto va en claro y además puede explotarse en fuerza bruta. Por tanto, para evitar la falta de seguridad en las transmisiones (con cifrado y autenticación), se ha creado una capa o parche complemento a SNMPv1 y v2 llamado versión v3, que añade a los mensajes SNMP (v1 y v2) una cabecera adicional.

Si no se dispone de seguridad suficiente, carácter general es aconsejable deshabilitar la ejecución de comandos SET por temas seguridad.

Mejoras en SNMPv2

Operaciones con grandes volúmenes: se incorpora una PDU *GetBulkRequest*. Esta PDU proporciona a las estaciones administradoras la posibilidad de trabajar con grandes cantidades de datos, de una sola vez, como grandes tablas.

Comunicación entre administradores: Inform_Request PDU, facilita la comunicación entre diferentes estaciones administradoras, *permitiendo la existencia de jerarquías que son necesarias en sistemas muy complejos.*

Mejoras en las adquisiciones: en version 1 cuando una de las variables en la lista de un comando GET fallaba, hacia que todo el comando fallara, obligando a eliminar esta variable de la lista y volver a consultar. En SNMPv2 este procesamiento es automático, y el error se indica en el valor de retorno de la variable.

Mejoras en monitorización remota: en redes que no están conectadas directamente a la estación de administración.

Otras redes, otros segmentos.

Comentario a la monitorización

SNMP gestiona dispositivos individuales, pero no permite diagnosticar fallos en un red remota u otro segmento de red.

Para ello, **el software de monitorización debe trasladarse a cada segmento de red**.

Esto se puede resolver mediante el uso de agentes en los segmentos remotos de red, utilizando equipos especiales o bien ordenadores de propósito general, llamados **sondas RMON (Remote MONitor)**

RMON Remote Monitor

Una de las mejoras principales de SNMP se denomina **Monitoreo Remoto (RMON).**

Las extensiones de RMON a SNMP **brindan la capacidad para observar la red como un todo, aunque esté distribuida,** en contraste con el análisis de dispositivos individuales, declarándose para ello una MIB especial para guardar información de monitorización de un segmento de red diferente. **La MIB asociada es 1.3.6.1.2.1.16**

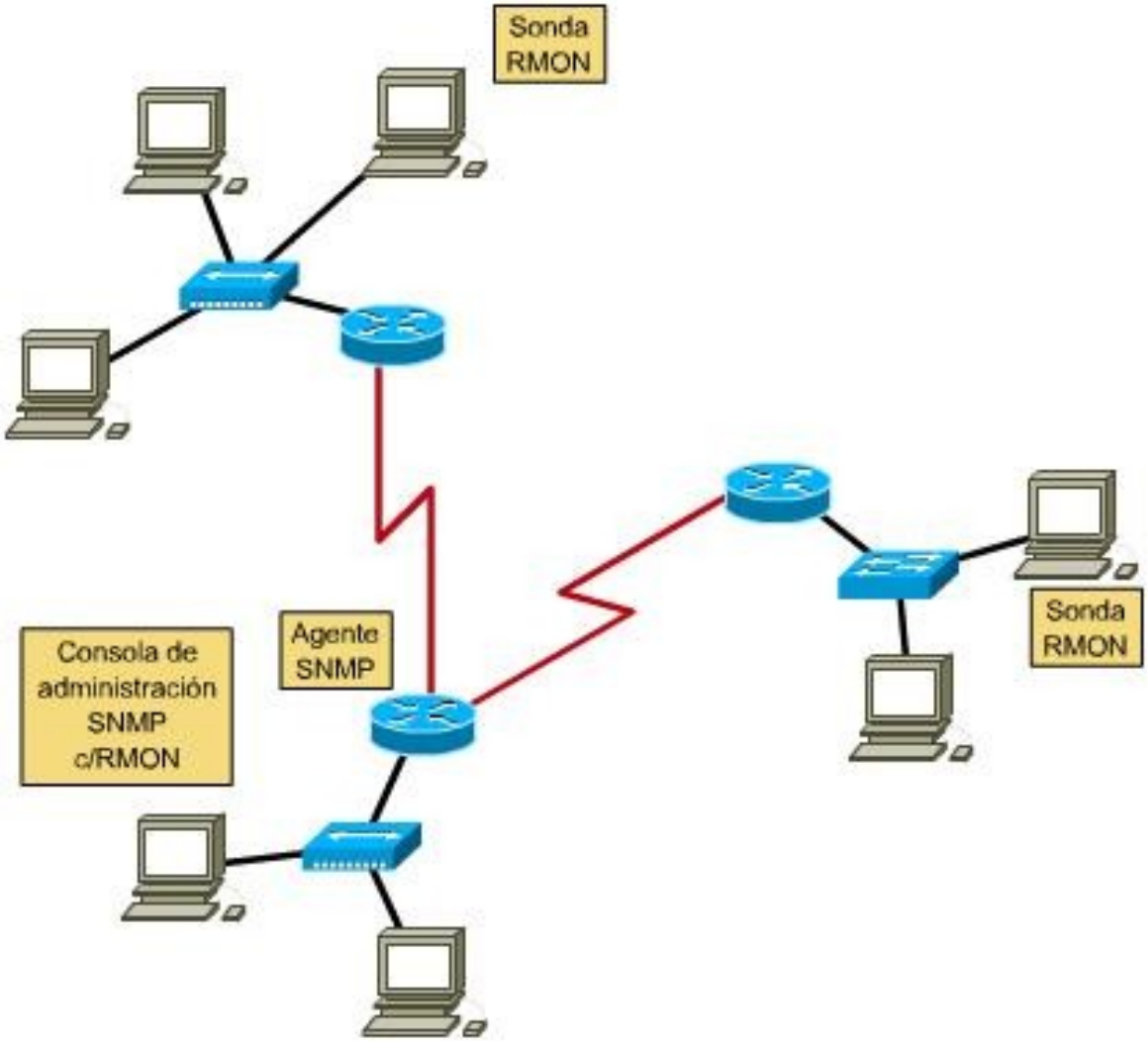
Las sondas RMON recopilan información y tiene la misma función que un agente SNMP, transmitiendo la información periódicamente. Además, pueden procesar la información a enviar a la estación de administrador.

La RMON está localizada en cada segmento de red y pueden introducirse en un host, en un switch, en un router o en un dispositivo específico para ello. Además, permite añadir **redundancia** a la administración de la red, ya que RMON permite volcar los datos a varias consolas de administración.

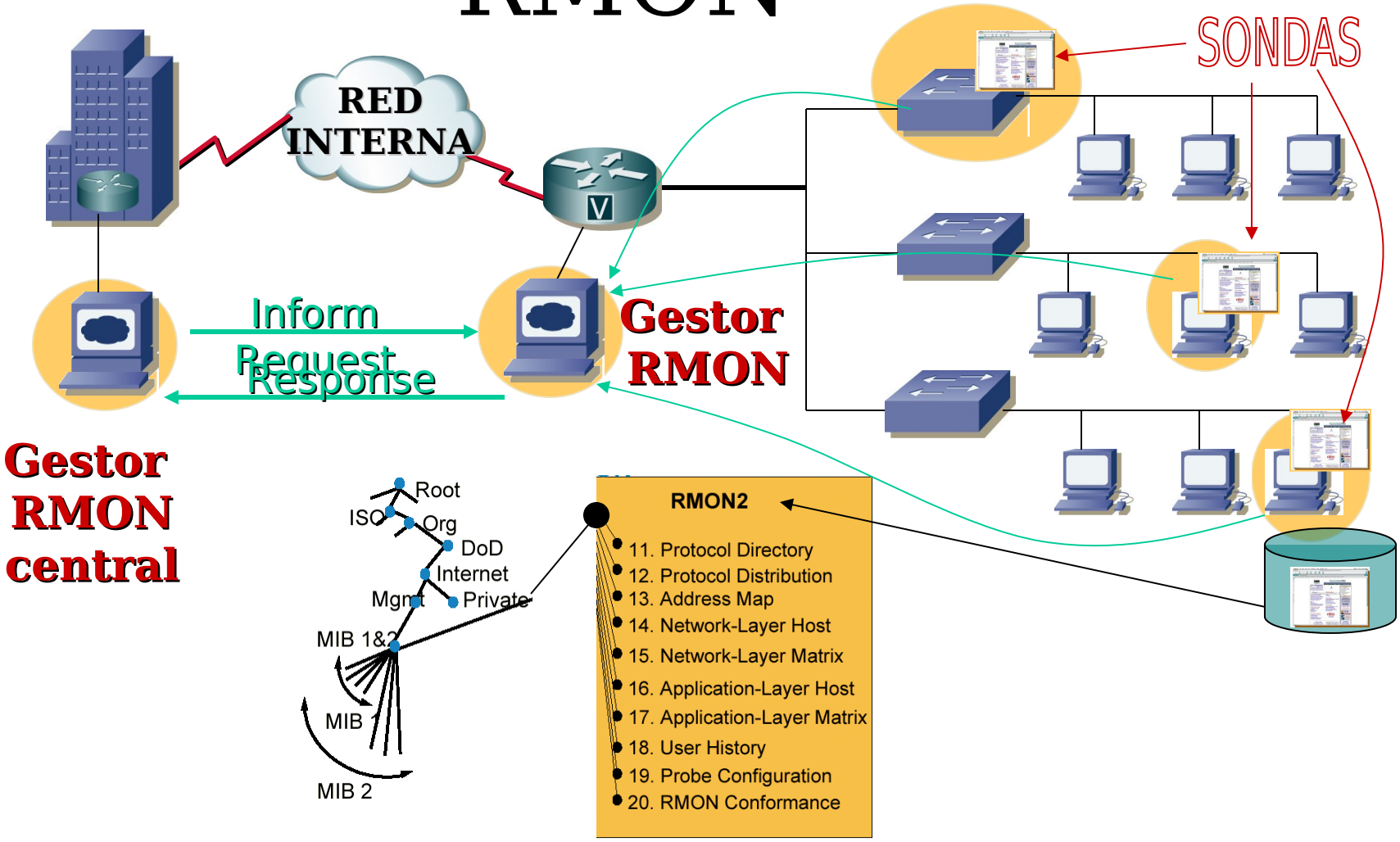
La **RMON1** trabaja en información de capa 1 y 2.

La **RMON2** trabaja en información de capa 3 y superiores.

Red con sondas RMON



Funcionamiento de RMON



Ejemplo de consulta SNMP (*snmpget*) (1/2)

"snmpget dominio comunidad OID"

donde *dominio* es la dirección IP de la máquina a conectar, *comunidad* (que por defecto tiene dos nombres: pública o privada) y en una notación intermedia entre ASCII y ASN1, especificamos el OID (*Object Identifier*).

Por ejemplo:

Snmpget 147.156.1.1 public iso.org.dod.internet.mgmt.mib_2.ip.ipDefaultTTL

Ejemplo de consulta SNMP (*snmpget*) (2/2): cálculo de la utilización de la interface de un router

La utilización de un interface se define como:

*(numero de bits procesados en ΔT)/((ΔT)*velocidad)*

es decir los bits mandados, frente a los bits que hubiese podido mandar si la utilización hubiese sido de 1 en un tiempo T.

Las variables a procesar son *ifInOctets, ifOutOctets* y *ifSpeed,* sobre el puerto correspondiente del router.

MRTG: Multi Router Traffic Grapher (1/2)

Multi Router Traffic Grapher (MRTG) es una herramienta para monitorización de tráfico en las redes y sus enlaces tanto internos como externos.

MRTG genera páginas HTML con imágenes PNG, que ofrecen una visión en tiempo real del tráfico.

MRTG está escrito en el Perl y C y trabaja bajo UNIX y el NT.

MRTG: Multi Router Traffic Grapher (2/2)

MRTG es un script en Perl que utiliza SNMP para leer cualquiera de los atributos de los objetos (contadores) de los routers y un programa rápido en C que procesa la información para visualizarla gráficamente en tiempo real.

Además, MRTG guarda la información por semanas, meses y años, monitorización hasta 200 enlaces.

MRTG se utiliza generalmente para monitorizar la carga del sistema, sesiones establecidas, tráfico, errores, etc

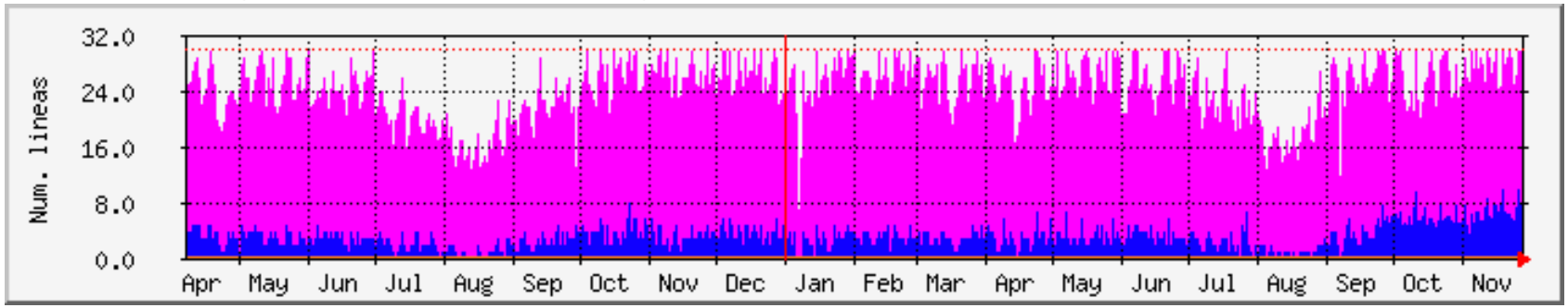
EJEMPLO DE MRTG: Esta página muestra el numero de líneas ocupadas en el servidor de acceso telefónico de la Universitat: annexy. Annexy dispone de un primario RDSI (30B+D), con 30 líneas disponibles para conexiones vía modem Las estadísticas se ejecuten cada 5 minutos.

Numero de lineas ocupadas de servidores annexy

Sistema: annexy.uv.es

Máximo esperado: 30

`Yearly' Graph (1 Day



BLUE ### Líneas ocupadas en annexy

VIOLET### Máximo de líneas ocupadas en annexy

MRTG MULTI ROUTER TRAFFIC GRAPHER

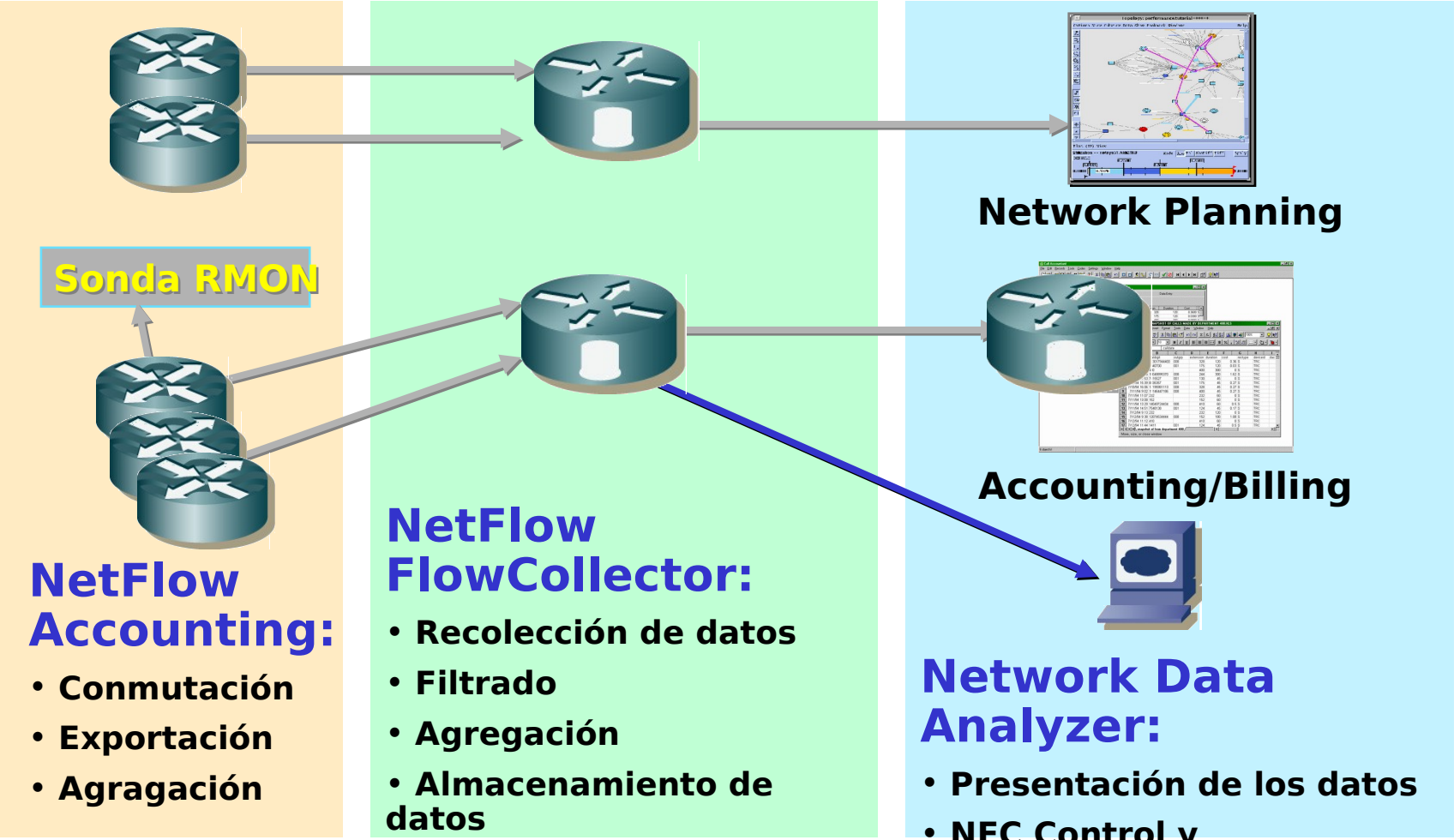
Instalación de MRTG

MRTG es de libre distribución y debe ser utilizado bajo los términos de *GNU General Public License*.

Para la descarga de la aplicación:

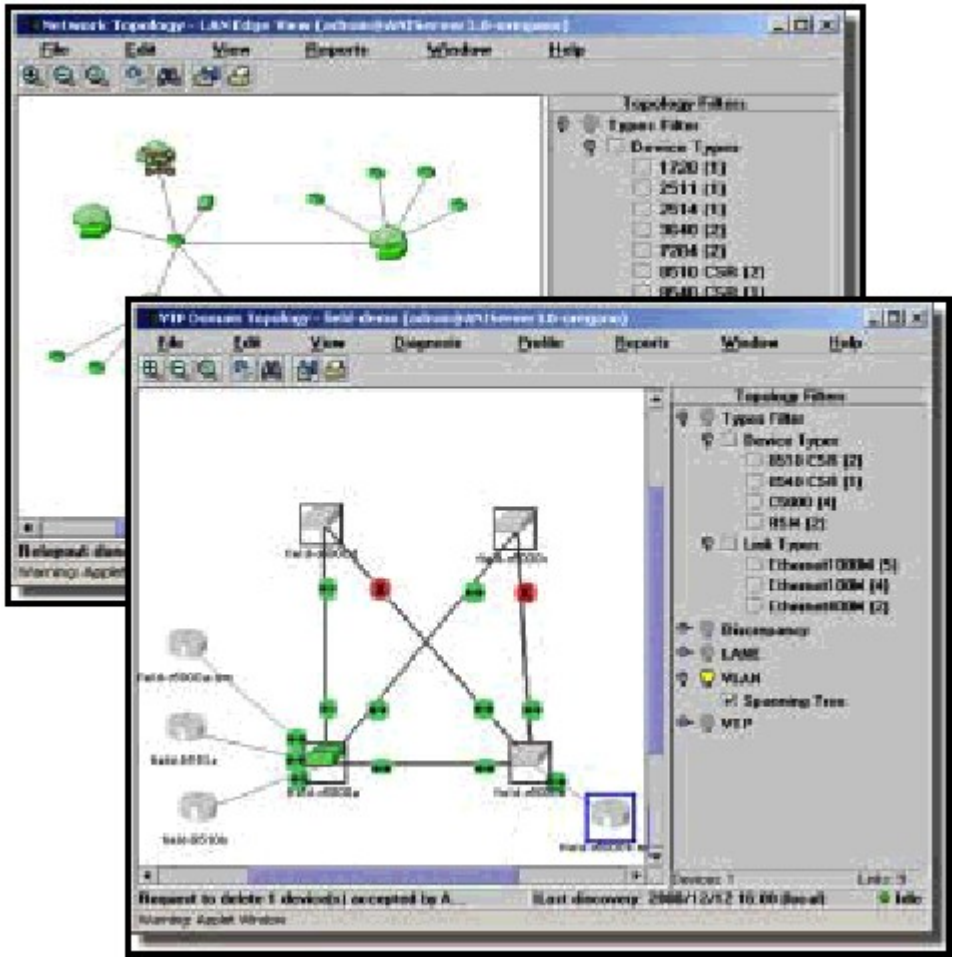
http://www.mrtg.org/

Aplicación SNMP: Netflow



Aplicación SNMP: CiscoWorks 2000

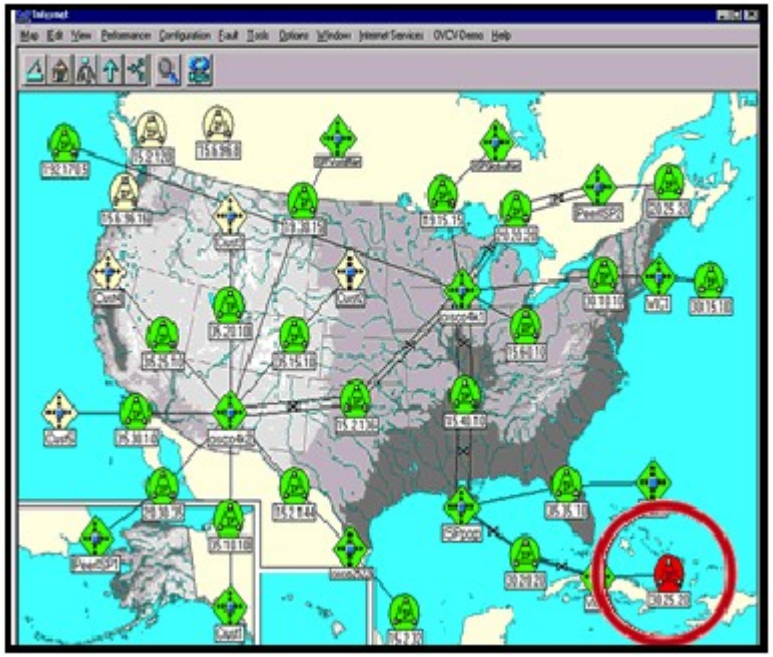
- Permiten ver la configuración
- Muestran la topología de la red
- Facilita la obtención de reports
- Permite actualizar IOS y descubrir nuevas versiones.

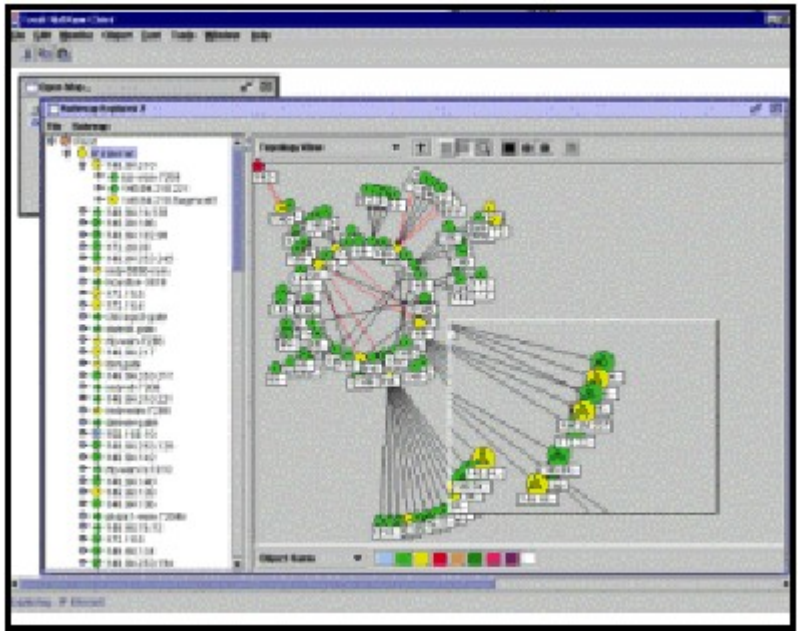


Extensiones:

- Cisco View.
- PIX Management.
- IDS Management.
- Router Management.
- Security Monitor Center
- Wireless LAN solution Engine

Aplicación SNMP: otros

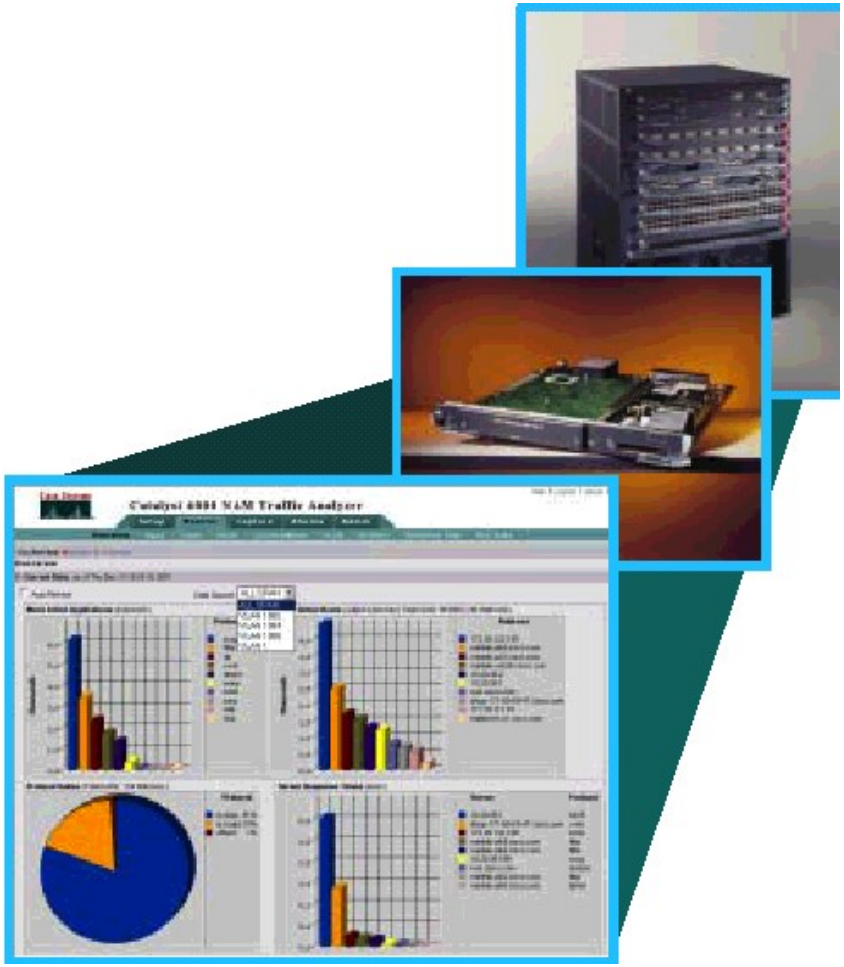




Monitores Hardware

Solución disponible en Cisco Catalyst 6500 y Catalyst 6000 series

Monitorización en tiempo real del tráfico de forma intensiva



RFCs

- RFC 1155 (SNMPv1 y SMI) y RFC 1157: SNMPv1
- RFC 1902 (SNMPv2 y SMI), RFC 1441 HASTA RFC 1452: SNMP VERSION 2
- RMON1: RFC1271
- RMON2: RFC2021, 2034
- RFC 2570-2576: SNMPv3